Secret sharing schemes for Multipartite access structures

Appala Naidu Tentu
C. R. Rao Advanced Institute of Mathematics, Statistics and Computer Science, University of Hyderabad Campus, Hyderabad, India.

V. Kamakshi Prasad
Department of Computer Science and Engineering, JNTU Hyderabad, Hyderabad, India.

V. Ch. Venkaiah
School of Computer and Information Sciences, University of Hyderabad, Hyderabad, India.

Abstract
Information security has become much more important since electronic communication is started to be used in our daily life. The content of the term information security varies according to the type and the requirements of the area. Secret sharing schemes are introduced to solve the problems for securing sensitive information. In this paper, we review our proposed hierarchical and compartmented secret sharing schemes. Later ideal and perfect disjunctive hierarchical secret sharing scheme, constructed based on the Maximum Distance Separable (MDS) codes, is proposed in this paper. The scheme is ideal as well as perfect. Also, size of the ground field for the proposed scheme is independent of the parameters of the access structure. Further, it is efficient and require O(n^3), where n is the number of participants.

Keywords: Secret sharing, Compartmented access structure, Disjunctive access structure, Conjunctive access structure, MDS code

Introduction
Secret sharing is a cryptographic primitive, which is used to distribute a secret among participants in such a way that an authorized subset of participants can uniquely reconstruct the secret and an unauthorized subset can get no information about the secret in the information theoretic sense. It is a fundamental method used in secure multiparty computations, where various distrusted participants cooperate and conduct computation tasks based on the private data they provide. A secret sharing scheme is called ideal if the maximal length of shares and the length of the secret are identical. Secret sharing was first proposed independently by Blakley [5] and Shamir [23]. The scheme by Shamir relies on the standard Lagrange polynomial interpolation, whereas the scheme by Blakley is based on the geometric idea that uses the concept of intersecting hyper planes.

The family of authorized subsets is known as the access structure. An access structure is said to be monotone if a set is qualified then its superset must also be qualified. Several access structures are proposed in the literature. They include the (t, n)-threshold access structure, the Generalized access structure and the Multipartite access structure. In (t, n)-threshold access structure there are n shareholders, an authorized group consists of any t or more participants and any group of at most t-1 participants is an unauthorized group. Let U be the set of n participants and let 2^U be its power set. Then 'Generalized access structure' refers to situations where the collection of permissible subsets of U may be any collection \( \Gamma \subseteq 2^U \) having the monotonicity property. In multipartite access structures, the set of players U is partitioned into m disjoint entities U_1, U_2, ..., U_m is called levels and all players in each level play exactly the same role inside the access structure. Disjunctive hierarchical access structure is a multipartite access structure in which each level U_i is assigned with a threshold ti for 1 \leq i \leq m, and the secret can be reconstructed when there are at least ti shareholders who all belong to levels smaller than or equal to U_i. Formally,

\[ U^F = \{ V \subseteq U : |V \cap \bigcup_{i=1}^{U(t)} U_i | \geq t_i, \text{ for some } i \in \{1, 2, ..., 1\} \} \]

Whereas in conjunctive hierarchical access structure we have

\[ U^F = \{ V \subseteq U : |V \cap \bigcup_{i=1}^{U(t)} U_i | \geq t_i, \text{ for all } i \in \{1, 2, ..., 1\} \} \]

Whereas in Compartmented access structure such that all subsets containing at least t_i participants from U_i for every i, 1 \leq i \leq m, and a total of at least t_0 participants are qualified to reconstruct the secret. Formally

\[ U^F = \{ V \subseteq U : |V \cap \bigcup_{i=1}^{U(t)} U_i | \geq t_0, \text{ for every } i \in \{1, 2, ..., m\} \text{ and } |V| \geq t_0 \} \], where \( t_0 \geq \sum_{i=1}^{m} t_i \)

A secret sharing scheme is a perfect realization of \( \Gamma \) if for all \( A \in \Gamma \), the users in A can always reconstruct the secret and for all B not in \( \Gamma \), the users in B collectively cannot learn anything about the secret, in the information theoretic sense.

Related Work
A multi-secret sharing scheme is a extension of a shamir’s [15] secret sharing. In these [15], [2] schemes there are several problems occures like, in every secret sharing process
only one secret can be shared and this algorithms is the one-time use scheme.

Shamir [23] pointed out that a hierarchical variant of threshold secret sharing scheme can be constructed simply by assigning larger number of shares to higher level participants. However, such a solution can be easily seen to be not ideal.

Kothari [16] introduced a scheme that is a generalization of schemes of Blakley, Shamir, Bloom, and Karnin et al. [5,14,16,17]. This generalized scheme is used to arrive at a hierarchical scheme, which provides different levels of shares [16]. At each level a set of linear equations is to be solved to obtain the secret. The size of the set of linear equations to be solved is a function of the level.

The earliest disjunctive secret sharing scheme is due to Simmons [24, 3], which is not ideal [15]. It is also in efficient because the dealer needs to check, possibly exponentially, many matrices for non-singularity [3] [26].

Brickell [7] offered two schemes for the disjunctive case, both ideal [26]. Both the schemes are inefficient [15]. One of the schemes suffers from the same problem as that of Simmons', while the other scheme requires finding an algebraic number satisfying an irreducible polynomial over the finite field [26].

The multilevel threshold scheme by Ghodosi et al. [12] work only for small number of shareholders [18, 3]. Tassa [26] and Tassa and Dyn [27] proposed ideal secret sharing schemes, based on Birkhoff interpolation and bivariate interpolation respectively, for several families of multipartite access structures that contain the multilevel and compartmented ones. These schemes either require a large finite field with some restrictions in assigning identities to the users [3] [27] [26] [1] or perfect in a probabilistic manner [17].

Constructions of ideal secret sharing schemes for variants of the multilevel access structures and for some tripartite access structures have been given also in [2, 3, 13, 21, 10, 11]. The problem of secret sharing in hierarchical (or multilevel) structures, was studied under different assumptions also in [4, 8, 9, 25, 32].

Linear codes have been used earlier in some constructions of threshold schemes [20, 14, 19, 22]. Blakley and Kabatianski [6,33] have established that ideal perfect threshold secret sharing schemes and MDS codes are equivalent.

Our contribution

In this paper, first we review the proposed secret sharing schemes for compartmented and hierarchical access structures. Later, ideal and perfect secret sharing is proposed for a disjunctive hierarchical access structure. The construction of this scheme is based on the maximum distance separable (MDS) codes. Novelty of our schemes is that it overcomes all the limitations present in most of the existing schemes. The size of the ground field, in our scheme, is independent of the parameters of the access structure and there are no restrictions in assigning identities to the participants. Our scheme is applicable for any number of participants. It is efficient and require $O(n^3)$, where $n$ is the number of participants, computation for setup, distribution, and recovery phases.

Organization of the paper

The rest of the paper is organized as follows: Section 2 presents some of the preliminaries used in the construction. Section 3 explains the overview of the previous proposed schemes given in [28,29,30,31]. Our proposed disjunctive scheme is described in section 4. In section 5, we discussed about privacy and performance analysis of proposed scheme and conclusions are in section 6.

Preliminaries

MDS codes

A linear block code over a field $F_q$ is a linear subspace of $F_q^n$, where $n$ is the block length of the code. More generally, a block code $C$ of length $n$ with $qk$ code words, is called a linear $[n,k]$ code if and only if its $qk$ code words form a $k$-dimensional subspace of the vector space of all $n$-tuples over the field $F_q$. An $[n,k,d]$ block code over $F_q$ is called Maximum Distance Separable (MDS) code if distance $d = n-k+1$. Two important properties, namely,

- Any $k$ columns of a generator matrix are linearly independent and
- Any $k$ symbols of a code word may be taken as message symbols,

of MDS codes have been exploited in the construction of our schemes. It may be noted that for any $k$, $1 \leq k \leq q-1$, and $k \leq n \leq q-1$ there is an $[n, k, n-k+1]$ MDS code and an $[q, k, q-k+1]$ extended Reed Solomon code.

Secret Sharing Scheme

The first idea of secret sharing schemes was independently introduced by Shamir [23] and Blakley [5]. A secret sharing scheme starts with a secret and then derives from it certain shares (or shadows) which are distributed to users. The secret may be recovered only by certain predetermined groups. More exactly, let $U$ be the set of $n$ users labeled with the numbers $1, ..., n$ and let us consider a set of authorized groups $\Gamma \subseteq 2^U$. Informally, a secret sharing scheme is a method of generating($S(I_1, I_2,..., I_q)$) such that

- Correctness: for any $A \in \Gamma$ the problem of finding the element, given the set($I_i | i \in A$), is "easy".
- Security: for any $A \in \tau$, the problem of finding the element, given the set($I_i | i \in A$), is "hard".

$S$ will be referred to as the secret and $I_1, I_2,..., I_n$ will be referred to as the shares (or the shadows) of $S$. The set from where the secrets are chosen will be denoted by $S$ or by $S_0$ and the set of the shares assigned to the $i^{th}$ user will be denoted by $S_i$, for all $1 \leq i \leq n$. Sometimes, it will be useful to consider the set of all possible shares. We will denote this set by $S_{shares}$.

Multipartite Secret Sharing Schemes

Compartmented schemes based on MDS codes

Perfect Compartmented Scheme:

Overview of our (T A Naidu et.al [30, 31]) proposed perfect compartmented secret sharing scheme given in section 2, in [31] as follows.
Let $s$ be the secret. Choose uniformly randomly $m + 1$ partial secrets $s_1, s_2, \ldots, s_m$ and $s'$ such that the secret is the sum of all these partial secrets, i.e., $s_1 + s_2 + \ldots + s_m + s'$. Select an $[n + 1 + k', k'' + 1, n + 1 + k' - k'']$ MDS code $C_1$ and also another MDS code $C_2$ with parameters $[2N-k, N, N-k+1]$, where Pick randomly and uniformly $i = 1, 2, \ldots, n$ shares $v_{ij}$ and $w_{ij}$, $1 \leq i \leq m, 1 \leq j \leq n_i$. Now choose code word of $C_{1i}$, $1 \leq i \leq m$, from the code $C_1$ and a codeword $C_{2i}$ from the code $C_2$. The choice of the codeword $C_{ni}$, $1 \leq i \leq m$, is such that the first component is the partial secret $s_i$, next $n_i$ components are the shares $v_{ij}$, $1 \leq j \leq n_i$, of the $i$th component, and the rest of the components are arbitrary. $k' - k_i + 1$ of these arbitrarily chosen components are made public corresponding to the codeword $C_{1i}$ so that if any $k_i$ participants from the $i$th compartment cooperate they can recover the first component, $s_i$, of this codeword, which is the $i$th partial secret. In a similar way, codeword $C_{2i}$ is chosen in such a way that the first component is the partial secret $s_i$, next $n_i$ components are the shares, $w_{ij}$, $1 \leq j \leq n_i$, of the first compartment, next $n_2$ components are the shares, $w_{2j}$, $1 \leq j \leq n_2$, of the second compartment and so on and the remaining components are arbitrary. As in the previous case these arbitrarily chosen components are made public so that if any $k$ of the participants cooperate they can recover the partial secret $s_i$.

**Computationally Perfect Scheme:**

We presented another compartmented secret sharing scheme in [31] using MDS codes which is improved version of above scheme, overcomes the shortcoming present in the scheme and hence is ideal. It is computationally perfect and relies on the hardness assumption of one way functions. Overview of our proposed computationally perfect compartmented secret sharing scheme given in [30, 31] as follows. This scheme uses only one MDS code, overcomes the shortcoming present in the first scheme and hence is ideal. It is computationally perfect and relies on the following hardness assumption.

**Assumption**

Let $a \in F_q$ and $f_i : F_q \to F_q, 1 \leq i \leq 2$, be two distinct one-way functions. Also, let $f_i(a) = b_i, 1 \leq i \leq 2$, then the computation of $a$ from the knowledge of either $b_1$ or $b_2$ is computationally hard.

Let $U, m, U_i, n_i, k_i, 1 \leq i \leq m, k, k', k''$ and $n$ be as in the previous scheme. Also, let $f_i : F_q \to F_q, 1 \leq i \leq 2$, be two distinct one-way functions.

**Overview of the Scheme:**

Let $s$ be the secret. Choose two one-way functions $f_1$ and $f_2$. As in the previous scheme, choose randomly and uniformly $m + 1$ partial secrets $s_i, 1 \leq i \leq m$, and $s'$ such that the secret is the sum of all partial secrets, i.e., $S = \sum_{i=1}^{m} s_i + 1$.

A way of choosing the $i^{th}, 1 \leq i \leq m$, codeword is as follows:

- Choose an $N$-vector whose first component is $s_i$, $i^{th}$ partial secret in the sum of the secret, next $n_i$ components are $v_{i1}, v_{i2}, \ldots, v_{in_i}$ (images of the shares of the $i^{th}$ compartment participants under the one-way function $f_1$ and rest of the components arbitrary.
- Reduce the generator matrix using elementary row operations so that the columns starting from $(\sum n_j + 2)^{th}$ column to $(\sum n_j + 1)^{th}$ column from a partial identity matrix.
- Multiply the reduced generator matrix with the $N$-component vector that was constructed above.

**Construction of the codeword $C$** is also similar. That is,

- Construct an $N$-component vector by taking the first component as $s$ next $n_i$ components as $v_{i1}^2, v_{i2}^2, \ldots, v_{in_i}^2$ followed by the $n_2$ components $v_{21}^2, v_{22}^2, \ldots, v_{2n_2}^2$ and so on up to the $n_m$ components $v_{m1}^2, v_{m2}^2, \ldots, v_{mn_m}^2$ of the $m^{th}$ component. By the way
- $v_{ij}^2, 1 \leq i \leq m, 1 \leq j \leq n_i$ is the image of the share of the $j^{th}$ participant in the $i^{th}$ compartment under the second one-way function $f_2$.
- Reduce the generator matrix using elementary row operations so that the first $N$ columns from the identity matrix.
- Multiply the reduced generator matrix with the $N$-component vector that was constructed above.

Distribute $v_{ij}, 1 \leq i \leq m, 1 \leq j \leq n_i$ to the $j^{th}$ participant in the $i^{th}$ compartment. Publicise $\sum_{j=1}^{n_i} u_{ijk}^{(i)}$ of $u_{ijk}^{(i)}$, $1 \leq j \leq m, j \neq i, 1 \leq k_i \leq n_i$ as public shares corresponding to $C_i, 1 \leq i \leq m$. Similarly, publicise $u_{m+2,j}, 1 \leq j \leq \sum_{j=1}^{m} n_j - k + 1$, as public shares corresponding to the codeword $C$.

If at least $k$ players such that at least $k_i$ of the form $i^{th}, 1 \leq i \leq m$ compartment participate then the secret can be recovered. The steps for recovery phase is given in

**Conjunctive Hierarchical scheme based on MDS Codes**

We present overview of secret sharing scheme with conjunctive hierarchical access structures given in [28, 29]
Proposed Disjunctive Secret Sharing Scheme

Overview of the Scheme:
The dealer considers an \([n, N, n-N+1]\) MDS code \(C\) over \(F_q\) and chooses \(m\) codeword’s. The choice of the \(t\)-th of these arbitrarily chosen components of the \(i\)-th codeword are made public so that if any \(t_i\) participants from the first \(i\) levels cooperate they can, with the help of the \(N-t_i\) public shares, reconstruct the \(i\)-th codeword uniquely and hence can recover the first component, \(s_i\), of this codeword, which is a term in the sum of the partial secrets.

Setup and Distribution
1. Select an \([n, N, n-N+1]\) MDS code \(C\) over \(F_q\) and choose \(m\) codeword’s as \(C_1, C_2, \ldots, C_m\), where the components from 2 to \(n+1\) corresponds to the second level and so on.

Note: A way of choosing a code word is as follows: Construct an \(N\)-vector whose first component is secret \(s\) followed by \(V_{11}, V_{12}, \ldots, V_i \sum_{j=1}^i nj\) and rest of the components are arbitrary. Reduce the generator matrix using elementary row operations so that the first \(N\) columns form the identity matrix. Multiply the above \(N\)-vector with the reduced generator matrix to arrive at the desired codeword.

2. Distribute \(V_{ij}, 1 \leq i \leq m, 1 \leq j \leq n\), as the share of the \(j\)-th player in the \(i\)-th compartment.
3. Publish \(U_{ij}, j \in S_i\) as the public shares corresponding to \(C_i\), where \(S_i \subseteq \{1: \sum_{k=1}^i nk + 2 \leq 2N-t_m\}\). Let \(S_i = N-4t\).
4. Also make the generator matrix \(G\) of the \([n, N, n-N+1]\) MDS code public.

Recovery Phase
If at least \(t_i\), \(1 \leq i \leq m\), players come from the first \(i\) levels, the secret \(s\) can be recovered. Assume that \(j_k\), \(1 \leq k \leq i\), is the number of players from the \(k\)-th level participating in the recovery phase. Also, let \(l_{1,1}, l_{2,1}, \ldots, l_{k,1}\) be the indices of the participants from the \(k\)-th level. Then the recovery phase consists of the following steps:

Form the codeword by multiplying the above reduced generator matrix with the message vector formed in step 2 of the recovery phase. Also, let \(L_{1,1}, L_{2,1}, \ldots, L_{i,1}\) be the indices of the participants from the \(i\)-th level. Then the recovery phase consists of the following steps:

1. Select \((N \sum_{k=1}^i j_k)\) shares from the list of public shares corresponding to \(C_i\). Let the indices of the selected shares be \(L_{1,1}, L_{2,1}, \ldots, L_{i,1}\).
2. Form the message vector from the shares of the participants who are co-operating in the recovery phase along with the selected public shares. Let this vector be \((v_1{l_{1,1}}, v_1{l_{2,1}}, \ldots, v_1{l_{1,1}}, v_2{l_{1,1}}, v_2{l_{2,1}}, \ldots, v_2{l_{1,1}}, \ldots, v_2{l_{1,1}}, v_1{l_{2,1}}, v_1{l_{3,1}}, \ldots, v_1{l_{1,1}}, \ldots, v_1{l_{2,1}}, v_2{l_{1,1}}, \ldots, v_2{l_{1,1}}, \ldots, v_2{l_{1,1}}, v_1{l_{3,1}}, \ldots, v_1{l_{1,1}}, \ldots, \)
3. Reduce, using the elementary row operations, the generator matrix \(G\) of the MDS code under consideration to another matrix that has the following structure:
   a) \((k_i + 1)\)th \(1 \leq t \leq j_i\), column of the generator matrix has 1 in the \(t\)-th row and zeros elsewhere,
   b) \((\sum_{k=1}^{t-1} n_j) + \sum_{k=1}^{t} l_k + 1\), \(1 \leq k \leq \sum_{k=1}^{t-1} n_j\), column of the generator matrix has 1 in the \((\sum_{k=1}^{t-1} n_j + 1)\)-th row and zeros elsewhere,
   c) \((\sum_{k=1}^i n_j) + \sum_{k=1}^{i+1} l_k + 1\), \(1 \leq t \leq (N \sum_{k=1}^i j_k)\), column of the generator matrix has 1 in the \((\sum_{k=1}^i n_j + 1)\)-th row and zeros elsewhere.
4. Form the codeword by multiplying the above reduced generator matrix with the message vector formed in step 2 of the recovery phase.
5. First component of the codeword is the secret to be recovered.

Privacy and Performance Analysis
This section analyzes the computational requirements and discusses the correctness of the proposed scheme.

Correctness of the Scheme
Following theorems establish that the proposed scheme is ideal and always recovers the secret if and only if the set of participants is an authorized set.
Theorem 1.
The secret can be recovered by the recovery phase described above if and only if the set of participants recovering the secret is an authorized set.

Proof: 
It can be seen that any N shares can reconstruct the code word C, for any i, 1 ≤ i ≤ m. This is because in an [n, k, d] MDS code any k symbols can be treated as message symbols. So, if \( \sum_{k=1}^{n} jk \), for any i such that 1 ≤ i ≤ m, players cooperate they can recover the secret s with the help of \( (N-\sum_{k=1}^{n} jk) \), public shares, whereas less than N shares cannot recover the secret s. This is because any N columns are linearly independent. So, the first column of the generator matrix, which corresponds to the secret s, is not in the span of less than N columns of the generator matrix. Therefore, the secret can be recovered only by an authorized set and not by an unauthorized set.

Theorem 2.
The proposed scheme is ideal.

Proof: 
As can be visualized from the scheme each participant is given exactly one share. Also, the space of secrets and the space of shares is \( F_q \). So, the proposed scheme is ideal.

Theorem 3.
The probability that an unauthorized set being able to recover the secret is equal to that of the exhaustive search, which is 1/q.

Proof: 
If less than \( t_i \), say \( k_n \), players cooperate from the first i, 1 ≤ i ≤ m, levels then with \( N-t_i \) public values the unauthorized set can only know \( N-t_i-k_n \) components of the codeword \( C_n \), for any i such that 1 ≤ i ≤ m. This leaves \( t_i-k_n \) degrees of freedom to determine a code word. So, there are \( q^{t_i-k_n} \) codewords that match with the \( N-t_i-k_n \) components in their positions. Among these, \( q^{t_i-k_n} \) codewords contain s as their first component. This is because in an [n, k, d] MDS code any k symbols can be treated as the message symbols and hence the first component of a codeword in code \( C_n \), 1 ≤ i ≤ m, which corresponds to s, is the weighted sum of the N message symbols. From the discussion above this sum consists of \( t_i-k_n \) unknowns. So, \( t_i-k_n \) degrees of freedom together with a linear constraint become \( (t_i-k_n)-I \) degrees of freedom. Thus, the probability that less than \( t_i \), 1 ≤ i ≤ m, players being able to recover the secret s is \( (q^{t_i-k_n}/q^{t_i-k_n}) \).

Complexity Analysis
In our computational requirements of Setup, Distribution and Reconstruction phases of the above proposed scheme are as follows: Assuming that the Vandermonde matrix is chosen as the generator matrix of the code, it can be seen that the reduction of each element requires at most \( 2 log n \), where n is the size of the largest exponent operations. So, reduction of all the elements of the generator matrix requires \( 2N n log n \) operations. Assuming that a code word is selected by specifying an N component vector and multiplying the resulting vector with the generator matrix, the code word selection in Step 1 requires \( 2N n m \) operations. Distribution and publishing in Steps 2, 3, and 4 requires no computation. So, the computational requirements of the Setup and Distribution phase is \( 2N n log n + 2N m \) operations. Steps 1 and 2 of the recovery phase select public values and form the message vector. This involves no computation. Reduction of generator matrix to the required form in Step 3 can be achieved in \( (2n(N-1)+n)N \) operations, here \( (2nN-n) \) operations to bring one column to a column of the identity matrix and there are N columns of the identity matrix, and to form the code word by multiplying the reduced generator matrix, it requires \( 2N n \) operations.

Comparison with existing schemes

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Ideal</th>
<th>Perfect</th>
<th>Works for small primes</th>
<th>No. of Share holders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simmons</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Large</td>
</tr>
<tr>
<td>Tassa</td>
<td>Yes</td>
<td>Yes (Prob)</td>
<td>No</td>
<td>Large</td>
</tr>
<tr>
<td>Belenky</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Large</td>
</tr>
<tr>
<td>Ours</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Large</td>
</tr>
</tbody>
</table>

Conclusion
We have proposed an ideal and perfect secret sharing is proposed for a disjunctive hierarchical access structure. The scheme is based on MDS codes and the constructions exploit some of the important properties of these codes. The proposed scheme overcomes all the limitations present in most of the existing schemes. The size of the ground field in our scheme is independent of the parameters of the access structure and there are no restrictions in assigning the identities to the participants. Our scheme is applicable for any number of shareholders. It is efficient and require \( O(n^3) \), where n is the number of participants, operations.

References